UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/663,891	09/18/2000	Robert Chojnacki	N0064US	4137

37583 7590 05/15/2008

NAVTEQ NORTH AMERICA, LLC
425 West RANDOLPH STREET
SUITE 1200, PATENT DEPT
CHICAGO, IL 60606

EXAMINER	
KHOSHNOODI, NADIA	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
05/15/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/663,891	CHOJNACKI, ROBERT	
	Examiner	Art Unit	
	NADIA KHOSHNOODI	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 November 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6,8,9,11-23 and 25-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6,8,9,11-23 and 25-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 September 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/11-05-2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/5/2007 has been entered.

Response to Amendment

Claims 5, 7, 10, and 24 are cancelled. Applicant's arguments/amendments with respect to the pending claims filed 11/5/2007 have been fully considered but they are not persuasive.

Response to Arguments

Applicants contend that the combination of Chan and Shear "do not teach a method for securely delivering a data product that is then usable without further decryption by the user." Examiner respectfully disagrees. Shear et al. was relied upon to teach/suggest the portion Applicants are referring to with the claim amendment introduced (i.e. "wherein said combined product is not cryptographically secured on the computer-readable storage medium"). Specifically, Shear et al. teach that the embodiments disclosed **permit** securing of the data by using a number of techniques which included "cryptographic and/or protection information that is stored on the DVD medium" (par. 283). Therefore, Shear et al. allow for the data to be encrypted but do not require it as a part of every embodiment disclosed. Furthermore, Shear et

al. mention that keeping the technical/security features minimal is preferable in certain embodiments in order to **minimize cost and complexity** of these items that are mass produced for consumers (par. 278). Thus, although Shear provide a medium which may be used with cryptographic protection, it is not a required feature of every embodiment disclosed and therefore Shear et al. teach/suggest wherein said combined product is not cryptographically secured on the computer-readable storage medium (par. 278 and par. 283).

Due to the reasons stated above, the Examiner maintains rejections with respect to the pending claims. The prior arts of records taken singly and/or in combination teach the limitations that the Applicant suggests distinguish from the prior art. Therefore, it is the Examiner's conclusion that the pending claims are not patentably distinct or non-obvious over the prior art of record as presented.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-4, 6, and 25-39 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 1:

It is unclear which element is "obtaining an unencrypted second portion of said one of said data products from said second location." Claim 1 mentions that the user is located at the second location which contains the unencrypted second portions of said data products, therefore

it is confusing as to what element is receiving/obtaining this information. Examiner presumes that Applicants incorporated this limitation as a step to show that one of the data products is obtained from the stored group and in this case the Examiner further presumes that obtaining refers to the fact that it is sent to the storage/memory area of the end user who is within the bounds of the second location (i.e. a transfer from one memory area at the second location to another memory area at the second location).

As per claims 2-4, 6, and 25-39:

These claims are rejected by virtue of their dependency.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1, 3-4, and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan, US Patent No. 6,473,860 and further in view of McMullan Jr. et al., US Patent No. 5,654746 and Shear et al., US Pub. No. 2001/0042043.

As per claim 1:

Chan substantially teaches a method for on-line mass distribution of data products to end users, the method comprising: maintaining a first portion of each of said data products at a first location (col. 10, lines 52-67 and col. 11, lines 9-11), maintaining an unencrypted second portion

of each of said data products at a second location, wherein the second location is different from said first location (col. 10, lines 52-67 and col. 11, lines 1-2); for each of said end users, confirming the end user's entitlement to one of said data products (col. 11, lines 11-13); obtaining an unencrypted second portion of said one of said data products from said second location (col. 11, lines 1-5); after said step of confirming, obtaining an encrypted first portion of said one of said data products at said second location from said first location, obtaining a decryption key and using said decryption key to decrypt said encrypted first portion (col. 11, lines 9-20); combining said decrypted first portion of said one of said data products and said unencrypted second portion of said one of said data products, wherein said step of combining is performed at said second location, wherein said end user is located at said second location (col. 11, lines 39-45), and providing said combined first portion and second portion to said user, wherein the first portion of said data product comprises critical data that enables a program executed on a computing platform to use said data product including both the first portion and the second portion together for an intended purpose (col. 11, lines 39-45).

Not explicitly disclosed is wherein the first portion is stored/maintained in an encrypted form on the central server. However, McMullan Jr. et al. teach control information of digital data is maintained in encrypted form at a server archive in order maintain the data's confidentiality. Furthermore, storing/maintaining critical data in an encrypted form is and has been very well known in the art for quite some time now. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Chan to maintain/store the first portion of data at the first location in encrypted form as well. This modification would have been obvious because a person having ordinary skill in the art, at the

time the invention was made, would have been motivated to do so since McMullan Jr. et al. suggest that it is well known to protect data that is stored by encrypting the data before storing in col. 2, lines 8-18 and col. 8, lines 26-40.

Also not explicitly disclosed is storing said combined product on a portable computer-readable storage medium, wherein combined product is not cryptographically secured on the computer readable storage medium, and where said user accesses said combined product from said storage medium with said computer platform at a third location different from said first location and said second location. However, Shear et al. teach that the content may be combined and stored on a disk (e.g. DVD or CD) where the disk maintains control information indicating the user's entitlement rights as assessed prior to allowing the downloading step (par. 283). Furthermore, Shear et al. teach that the disk contents may be accessed via a computing platform which can communicate with another entity to continuously ensure that the entitlement rights are not being exceeded (par. 279). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Chan for the data product to be stored on a portable medium different from the locations that the data product is combined/downloaded at. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Shear et al. suggest that having the control information on the disk in addition to a secure node enables continuous observation that users are not exceeding the rights granted in the entitlement rights for that particular user/data product in 279.

As per claim 3:

Chan and McMullan Jr. et al. substantially teach the method of claim 1. Furthermore, Chan teaches wherein said data products include digital copies of movies (col. 10, lines 52-55).

As per claim 4:

Chan, McMullan Jr. et al., and Shear et al. substantially teach the method of claim 1. Furthermore, McMullan Jr. et al. teach wherein said data products include digital copies of musical songs (col. 3, lines 49-58).

As per claim 6:

Chan, McMullan Jr. et al., and Shear et al. substantially teach the method, as applied to claim l above. Chan teaches the method further comprising the step of prior to the step of combining, encrypting said first portion of one of said data products (col. 4, lines 25-33).

III. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chan, US Patent No. 6,473,860 and McMullan Jr. et al., US Patent No. 5,654746 and Shear et al., US Pub. No. 2001/0042043 as applied to claim 1 above, and further in view of Porter et al., United States Patent No. 5,845,067

As per claim 2:

Chan, McMullan Jr. et al., and Shear et al. substantially teach the method, as applied to claim 1 above. Not explicitly disclosed is the method, wherein said data products include geographic databases. However, Porter et al. teaches that a document can be any information stored as files in a file system, which can equate to the information contained by a geographic database. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Chan et al. for the data product to include files of geographical information stored in a file system, which is equivalent to a database. This

modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Porter et al. in col. 7, lines 26-32.

IV. Claims 8-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan, US Patent No. 6,473,860 and further in view of Shear et al., US Pub. No. 2001/0042043.

As per claim 8:

Chan teaches a system for secure on-line mass distribution of data products to end users comprising: an authorization server at a first location having associated therewith copies of first portions of a plurality of data products, wherein said first portions of the data products do not include information to enable encrypted data to be decrypted (col. 11, lines 11-13); a plurality of data distribution terminals at a plurality of locations different from said first location, each of said data distribution terminals has stored thereon copies of second portions of said plurality of data products (col. 10, line 52 – col. 11, line 4); a communications system that provides for exchange of data between the entity and said plurality of data distribution terminals (col. 11, lines 7-9), and a data distribution program that provides copies of said data products to those end users who are entitled to have said copies thereof (col. 11, lines 7-11); wherein said data distribution program provides a copy of a data product by combining a copy of the first portion of said data product obtained from said authorization server with a copy of the second portion of said data product obtained from one of said plurality of data distribution terminals, wherein said step of combining is performed at a location of said one of said plurality of data distribution terminals and said end user is located at said location of said one of said plurality of data distribution terminals (col. 11, lines 39-45) .

Not explicitly disclosed is a storing device interface associated with said data distribution terminal, wherein said storage device interface stores said combined product on a portable computer-readable storage medium, wherein combined product is not cryptographically secured on the computer readable storage medium, and wherein said user accesses said combined product from said storage medium with a computer platform at a location different from said location of said data distribution terminal. However, Shear et al. teach that the content may be combined and stored on a disk (e.g. DVD or CD) where the disk maintains control information indicating the user's entitlement rights as assessed prior to allowing the downloading step (par. 283). Furthermore, Shear et al. teach that the disk contents may be accessed via a computing platform which can communicate with another entity to continuously ensure that the entitlement rights are not being exceeded (par. 279). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Chan for the data product to be stored on a portable medium different from the locations that the data product is combined/downloaded at. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Shear et al. suggest that having the control information on the disk in addition to a secure node enables continuous observation that users are not exceeding the rights granted in the entitlement rights for that particular user/data product in 279.

As per claim 9:

Chan and Shear et al. substantially teach the system, as applied to claim 8 above. Furthermore, Chan teaches wherein said authorization server also has associated therewith an

authorization database containing data indicating entitlement by said end users to copies of said data products (col. 10, lines 24-45).

V. Claims 11-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan, US Patent No. 6,473,860 and Shear et al., US Pub. No. 2001/0042043, as applied to claim 8 above, and further in view of Ginter et al., United States Patent No. 6,237,786 and Shear et al., US Pub. No. 2001/0042043.

As per claim 11:

Chan and Shear et al. substantially teach the system as applied to claim 8. Furthermore, Chan teaches the system wherein the authorization server sends to the data distribution terminal the first portion in encrypted form that can be decrypted using a first decryption key (col. 11, lines 1-20). Not explicitly disclosed is an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to access the data product. However, Ginter et al. teach the system wherein the authorization server sends to the data distribution terminal the first portion in encrypted form that can be decrypted using a first decryption key and an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to access the data product (col. 14, lines 21-43 and col. 22, lines 13-45). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Chan as modified by Shear et al. to supply the terminal with a unique key pair so it can be verified that an entity authorized to access the data product is doing so. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ginter et al.

suggest verifying the entity accessing the data product is authorized cuts down on unauthorized access in col. 22, lines 13-45.

As per claim 12:

Chan, Shear et al., and Ginter et al. substantially teach the system as applied to claim 11. Furthermore, Ginter et al. teach the method/system wherein the second decryption key is derived as a function of an environmental parameter (col. 22, lines 13-45).

As per claim 13:

Chan, Shear et al., and Ginter et al. substantially teach the system as applied to claim 12. Furthermore, Ginter et al. teach the method/system wherein the environmental parameter comprises an identification code associated with the entity authorized to access the data product (col. 22, lines 13-45).

As per claim 14:

Chan, Shear et al., and Ginter et al. substantially teach the system as applied to claim 11. Furthermore, Ginter et al. teach the system wherein the data distribution terminal has access to the second decryption key and decrypts the encrypted authorization key and to thereby gain access to the verification information; and the third entity using the verification information to validate storage of the data product (col. 131, lines 18-44).

As per claim 15:

Chan, Shear et al., and Ginter et al. substantially teach the system as applied to claim 11. Furthermore, Ginter et al. teach the system wherein the data distribution terminal has access to the second decryption key and decrypts the encrypted authorization information, to thereby gain access to verification information, and to compare at least a portion of the verification

information to predetermined information associated with the user so as to determine whether the user is authorized to gain access to the data product (col. 131, lines 18-67).

As per claim 16:

Chan, Shear et al., and Ginter et al. substantially teach the system as applied to claim 15. Furthermore, Ginter et al. teach the system wherein the predetermined information associated with the user comprises an identification code (col. 131, lines 40-44).

As per claim 17:

Chan and Shear et al. substantially teach the system as applied to claim 8. Chan further teaches that the authorization server sends to the data distribution terminal the first portion in encrypted form that can be decrypted using a first decryption key (col. 11, lines 1-20). Not explicitly disclosed is wherein an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to access the data product. However, Ginter et al. teach the method/system wherein an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to access the data product (col. 14, lines 21-43 and col. 22, lines 13-45). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Chan as modified by Shear et al. to supply the terminal with a unique key pair so it can be verified that an entity authorized to access the data product is doing so. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ginter et al. suggest verifying the entity accessing the data product is authorized cuts down on unauthorized access in col. 22, lines 13-45.

As per claim 18:

Chan, Shear et al., and Ginter et al. substantially teach the system as applied to claim 17. Furthermore, Ginter et al. teach the system wherein the second decryption key is derived as a function of an environmental parameter (col. 22, lines 13-25).

As per claim 19:

Chan, Shear et al., and Ginter et al. substantially teach the system as applied to claim 18. Furthermore, Ginter et al. teach the system wherein the environmental parameter comprises an identification code associated with the entity authorized to store the data product (col. 22, lines 13-25).

As per claim 20:

Chan, Shear et al., and Ginter et al. substantially teach the system as applied to claim 17. Furthermore, Ginter et al. teach the system wherein the data distribution terminal has access to the second decryption key and decrypts the encrypted authorization key to thereby gain access to the verification information; and the third entity using the verification information, and to use the verification information to validate storage of the data product (col. 104, line 25 – col. 106, line 15).

As per claim 21:

Chan, Shear et al., and Ginter et al. substantially teach the system as applied to claim 17. Furthermore, Ginter et al. teach the system wherein the data distribution terminal has access to the second decryption key and decrypts the encrypted authorization information, to thereby gain access to verification information, and to compare at least a portion of the verification information to predetermined information associated with the storage medium so as to determine

whether the storage medium is authorized to gain access to store the data product (col. 78, lines 8-58).

As per claim 22:

Chan, Shear et al., and Ginter et al. substantially teach the system as applied to claim 21. Furthermore, Ginter et al. teach the system wherein the predetermined information associated with the storage medium comprises and identification code (col. 22, lines 13-45).

VI. Claims 25-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan, US Patent No. 6,473,860; McMullan Jr. et al., US Patent No. 5,654746; and Shear et al., US Pub. No. 2001/0042043, as applied to claim 1 above, and further in view of Ginter et al., United States Patent No. 6,237,786 and Shear et al., US Pub. No. 2001/0042043.

As per claim 25:

Chan, McMullan Jr. et al., and Shear et al. substantially teach the method as applied to claim 1. Furthermore Chan teaches sending to the second location, together with the encrypted first portion, an encrypted authorization key that can be decrypted using a second decryption key (col. 11, lines 1-20). Not explicitly disclosed is using a second decryption key so as to reveal verification information indicative of an entity authorized to access the data product. However, Ginter et al. teach the system wherein the authorization server sends to the data distribution terminal the first portion in encrypted form that can be decrypted using a first decryption key and an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to access the data product (col. 14, lines 21-43 and col. 22, lines 13-45). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Chan as modified

by Shear et al. to supply the terminal with a unique key pair so it can be verified that an entity authorized to access the data product is doing so. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ginter et al. suggest verifying the entity accessing the data product is authorized cuts down on unauthorized access in col. 22, lines 13-45.

As per claim 26:

Chan, McMullan Jr. et al., Shear et al., and Ginter et al. substantially teach the system as applied to claim 11. Furthermore, Ginter et al. teach the method/system wherein the second decryption key is derived as a function of an environmental parameter (col. 22, lines 13-45).

As per claim 27:

Chan, McMullan Jr. et al., Shear et al., and Ginter et al. substantially teach the method as applied to claim 26. Furthermore, Ginter et al. teach the method/system wherein the environmental parameter comprises an identification code associated with the entity authorized to access the data product (col. 22, lines 13-45).

As per claim 28:

Chan, McMullan Jr. et al., Shear et al., and Ginter et al. substantially teach the method as applied to claim 27. Furthermore, Ginter et al. teach the method wherein generating the second decryption key as the function of the identification code; using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and using the verification information to validate storage of the data product (col. 131, lines 18-44).

As per claim 29:

Chan, McMullan Jr. et al., Shear et al., and Ginter et al. substantially teach the method as applied to claim 25. Furthermore, Ginter et al. teach the method wherein a third set of logic executable by using the second decryption key to decrypt the encrypted authorization information, to thereby gain access to verification information, and using the verification information to validate use of the data product (col. 131, lines 18-67).

As per claim 30:

Chan, McMullan Jr. et al., Shear et al., and Ginter et al. substantially teach the method as applied to claim 29. Furthermore, Ginter et al. teach the method/system wherein using the verification information to validate use of the data product comprises comparing at least a portion of the verification information to predetermined information so as to determine whether the user is authorized to access the data product (col. 14, lines 21-43 and col. 22, lines 13-45).

As per claim 31:

Chan, McMullan Jr. et al., Shear et al., and Ginter et al. substantially teach the method as applied to claim 30. Furthermore, Ginter et al. teach the method wherein the predetermined information comprises an identification code (col. 131, lines 40-44).

As per claim 32:

Chan, McMullan Jr. et al., and Shear et al. substantially teach the method as applied to claim 1. Chan further teaches that the authorization server sends to the data distribution terminal the first portion in encrypted form that can be decrypted using a first decryption key (col. 11, lines 1-20). However, Ginter et al. teach the method further comprising using a second decryption key so as to reveal verification information indicative of an entity authorized to store the data product (col. 14, lines 21-43 and col. 22, lines 13-45). Therefore, it would have been

obvious to a person in the art at the time the invention was made to modify the method disclosed in Chan as modified by Shear et al. to supply the terminal with a unique key pair so it can be verified that an entity authorized to access the data product is doing so. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ginter et al. suggest verifying the entity accessing the data product is authorized cuts down on unauthorized access in col. 22, lines 13-45.

As per claim 33:

Chan, McMullan Jr. et al., Shear et al., and Ginter et al. substantially teach the method as applied to claim 32. Furthermore, Ginter et al. teach the method wherein the second decryption key is derived as a function of an environmental parameter (col. 22, lines 13-25).

As per claim 34:

Chan, McMullan Jr. et al., Shear et al., and Ginter et al. substantially teach the method as applied to claim 33. Furthermore, Ginter et al. teach the method wherein the environmental parameter comprises an identification code associated with the entity authorized to store the data product (col. 22, lines 13-25).

As per claim 35:

Chan, McMullan Jr. et al., Shear et al., and Ginter et al. substantially teach the method as applied to claim 34. Furthermore, Ginter et al. teach the method of generating the second decryption key as the function of the identification code; using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and using the verification information to validate storage of the data product (col. 104, line 25 – col. 106, line 15).

As per claim 36:

Chan, McMullan Jr. et al., Shear et al., and Ginter et al. substantially teach the method as applied to claim 32. Furthermore, Ginter et al. teach the method further comprising using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and using the verification information tot validate storage of the data product (col. 104, line 25 – col. 106, line 15).

As per claim 37:

Chan, McMullan Jr. et al., Shear et al., and Ginter et al. substantially teach the method as applied to claim 36. Furthermore, Ginter et al. teach the method wherein using the verification information to validate storage of the data product comprises comparing at least a portion of the verification information to predetermined information associated with the storage medium so as to determine whether the storage medium is authorized to gain access to store the data product (col. 78, lines 8-58).

As per claim 38:

Chan, McMullan Jr. et al., Shear et al., and Ginter et al. substantially teach the method as applied to claim 37. Furthermore, Ginter et al. teach the method wherein the predetermined information associated with the storage medium comprises and identification code (col. 22, lines 13-45).

VII. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chan, US Patent No. 6,473,860 and Shear et al., US Pub. No. 2001/0042043as applied to claim 8 above, and further in view of Ahrens et al., United States Patent No. 5,951,620.

As per claim 23:

Chan and Shear et al. substantially teach the system as applied to claim 8. Not explicitly disclosed is the system wherein the data product comprises geographic information. However, Ahrens et al. teach the use of a navigation system with geographic information. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Chan for the data product to be geographic information for a navigation system. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ahrens et al. in col. 7, lines 29-44.

VIII. Claim 39 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chan, US Patent No. 6,473,860; McMullan Jr. et al., US Patent No. 5,654746; and Shear et al., US Pub. No. 2001/0042043, as applied to claim 1 above, and further in view of Ahrens et al., United States Patent No. 5,951,620.

As per claim 39:

Chan, McMullan Jr. et al., and Shear et al. substantially teach the method as applied to claim 1. Not explicitly disclosed is the method wherein the data product comprises geographic information. However, Ahrens et al. teach the use of a navigation system with geographic information. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Chan for the data product to be geographic information for a navigation system. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ahrens et al. in col. 7, lines 29-44.

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 6,308,179
2. US Patent No. 5,917,908
3. US Patent No. 6,204,774
4. US Patent No. 6,297,891
5. US Patent No. 6,615,349
6. US Pub. No. 2001/0032088
7. US Pub. No. 2004/0039741

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nadia Khoshnoodi/
Examiner, Art Unit 2137
5/10/2008

NK

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137